AXIS Device Manager

Podręcznik użytkownika

Spis treści

Informacje o narzędziu AXIS Device Manager

AXIS Device Manager to oprogramowanie do instalacji i zarządzania przeznaczone do urządzeń Axis. Może ono automatycznie przeszukiwać sieć w poszukiwaniu urządzeń, przypisywać adresy IP, ustawiać hasła, pokazywać status połączeń oraz zarządzać aktualizacjami oprogramowania sprzętowego, certyfikatami i konfiguracją wielu urządzeń.

AXIS Device Manager obejmuje następujące komponenty:

- AXIS Device Manager Service Control — serwer obsługujący całą komunikację z urządzeniami Axis
- AXIS Device Manager Client — interfejs użytkownika, który umożliwia zdalne zarządzanie z poziomu Internetu lub sieci firmowej

Z tym samym serwerem może być połączonych kilku klientów. Klient może być połączony z wieloma serwerami jednocześnie.

Informacje o rozwiązaniu

Wymagania wstępne

Zgodne systemy operacyjne:

Wymagane: 64-bitowy system operacyjny, Microsoft .NET w wersji 4.8

Obsługiwany system operacyjny: Windows 10 Pro, Windows 11 Pro, Windows Server 2016, Windows Server 2019, Windows Server 2022

Zalecenia: Najnowsze dodatki Service Pack do systemu operacyjnego.

Minimalne zalecenia dotyczące systemu:

- Minimum (do 500 urządzeń): procesor Intel Core i5 lub odpowiednik, 4 GB RAM, 100 Mb/s w infrastrukturze sieciowej
- Zalecenie (500–2000 urządzeń): procesor Intel Core i7 lub odpowiednik, 8 GB RAM, 1000 Mb/s w infrastrukturze sieciowej
- Nie zaleca się przekraczania liczby 2000 urządzeń na serwer.
- Upewnij się, że urządzenia Axis zawierają najnowszą dostępną wersję systemu AXIS OS.

Uwaga

Zawsze wspieramy dwie poprzednie wersje najnowszego wydania. Szczegóły dotyczące obsługiwanych wersji są dostępne w informacjach o wersji.

Obsługiwane urządzenia:

Urządzenia AXIS z systemem AXIS OS w wersji 4.40 lub nowszej. (Należy pamiętać, że dokładne obsługiwane funkcje różnią się w zależności od konkretnego modelu produktu i oprogramowania sprzętowego)

Języki:

Interfejs użytkownika + pliki pomocy: angielski, francuski, niemiecki, włoski

Tylko interfejs użytkownika: arabski, chiński (uproszczony), chiński (tradycyjny), czeski, fiński, hiszpański, japoński, koreański, niderlandzki, perski, polski, portugalski (Brazylia), rosyjski, szwedzki, tajski, turecki i wietnamski.

Od czego zacząć

Instalowanie oprogramowania

Aby zainstalować narzędzie AXIS Device Manager 5, upewnij się, że masz pełne uprawnienia administratora na komputerze, na którym instalujesz to oprogramowanie, a następnie wykonaj następujące czynności:

1. *Przejdź na stronę produktu w witrynie axis.com i pobierz aplikację komputerową AXIS Device Manager*
2. Uruchom instalator i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Uwaga

Jeśli jeszcze nie została zainstalowana platforma Microsoft .NET 4.8, zostanie zainstalowana (znajduje się w pliku instalacyjnym). To potrwa kilka minut. Platformę Microsoft .NET 4.8 można również zainstalować za pośrednictwem usługi Windows Update przed przystąpieniem do instalacji narzędzia AXIS Device Manager.

Łączenie z serwerem

Po pierwszym uruchomieniu narzędzia AXIS Device Manager jest wyświetlany monit o połączenie z serwerem. Serwer może być uruchomiony na komputerze lokalnym lub na serwerze zdalnym.

Aby zalogować się jako lokalny użytkownik systemu Windows:

1. Wybierz **This computer (Ten komputer)**.
2. Zaznacz **Log on as current user (Zaloguj się jako bieżący użytkownik)**, aby się zalogować przy użyciu bieżących poświadczeń.

Aby zalogować się jako inny użytkownik na serwerze lub w domenie:

- Wybierz **Other user (Inny użytkownik)**.
- W sekcji **Other user (Inny użytkownik)** wprowadź poświadczenia odpowiedniego konta.
- Zaznacz **Remember me (Zapamiętaj mnie)**, aby pominąć ten krok przy następnym uruchomieniu klienta.
- Kliknij **Log on (Zaloguj się)**.

Uwaga

Aby wyczyścić zapisane poświadczenia dla wszystkich serwerów, przejdź do ekranu logowania i wybierz **Delete saved passwords (Usuń zapisane hasła)**.

Aby zalogować się do zdalnego serwera:

1. Wybierz opcję **Remote server (Serwer zdalny)**.
2. Wybierz serwer z listy rozwijanej albo wprowadź w polu adres IP lub DNS.
3. Wprowadź swoje poświadczenia
4. Kliknij **Log on (Zaloguj się)**.

Uwaga

Opcji tej nie można użyć w celu zalogowania się do zdalnego serwera z komputera, który nie należy do domeny Windows.

Połączenia z wieloma serwerami

Za pomocą narzędzia AXIS Device Manager można się połączyć z wieloma serwerami. Po pomyślnym zalogowaniu się na serwerze można się przełączać między serwerami w menu głównym.

1. Przejdź do menu głównego > Servers (Serwery) > New connection (Nowe połączenie)
2. Wybierz połączenie ze swoim komputerem lub serwerem zdalnym, jak opisano powyżej.

Konfiguracja początkowa

Aby rozpocząć, wykonaj następujące czynności:

- Dodaj urządzenia i utwórz konta użytkowników, patrz:
- Wzmocnij cyberbezpieczeństwo systemu. Patrz

Zarządzaj urządzeniami

Dodawanie urządzeń

AXIS Device Manager automatycznie przeszukuje sieć w poszukiwaniu podłączonych urządzeń i próbuje wykonać logowanie na wszystkich urządzeniach. Lista znalezionych urządzeń zawiera adres urządzenia (adres IP lub nazwę hosta), numer seryjny, model i status. Numer seryjny (S/N) jest wydrukowany na etykiecie produktu.

Aby dodać urządzenia z listy:

1. Wybierz urządzenia, które chcesz dodać, i kliknij **Next (Dalej)**.
2. Wybierz **Use host name when possible (Użyj nazwy hosta, jeśli to możliwe)**. Jeśli urządzenie zostanie dodane przy użyciu nazwy hosta, będzie ona używana we wszelkiej dalszej komunikacji z urządzeniem. Jeśli nazwa hosta nie będzie dostępna, zostanie użyty adres IP.
3. Ustaw hasło dla niemających go urządzeń. Jeśli nie należy ustawiać hasła, wybierz **Skip (Pomiń)**.
4. Kliknij **Next (Dalej)**.

Na stronie „Ready to add devices (Gotowość do dodania urządzeń)" wyświetlane są urządzenia, które mają zostać dodane.

5. Kliknij **Finish (Zakończ)**, aby dodać urządzenia.

Usuń urządzenia

Aby usunąć urządzenia z listy:

1. Przejdź do obszaru **Device management (Zarządzanie urządzeniami)**.
2. Zaznacz urządzenia.
3. Kliknij prawym przyciskiem myszy i wybierz **Remove (Usuń)**.
4. Kliknij **Tak**.

Zastępowanie urządzeń

Aby zastąpić urządzenie w narzędziu AXIS Device Manager, podłącz nowe urządzenie i ponownie zastosuj konfigurację z istniejącego urządzenia. Jeśli operacja się powiedzie, zastąpione urządzenie zostanie usunięte. Dla urządzenia tego musi być dostępny co najmniej jeden punkt przywracania, patrz . Do nowego urządzenia nie zostaną przeniesione żadne punkty przywracania.

1. Przejdź do obszaru **Device management (Zarządzanie urządzeniami)**.
2. Przejdź do paska narzędzi i kliknij ikonę zastępowania urządzenia.
3. Wybierz urządzenie do zastąpienia i kliknij **OK**.
4. Wybierz urządzenie, którym chcesz je zastąpić, i kliknij **OK**.
5. Kliknij **Next (Dalej)**, aby pobrać konfigurację urządzenia z ostatniego punktu przywracania.
6. Przejdź do obszaru **Parameters (Parametry) > Additional Settings (Ustawienia dodatkowe)** i wybierz parametry i ustawienia do zastosowania.
7. Kliknij **Next (Dalej)**.
8. Kliknij **Finish (Zakończ)**, aby zastosować ustawienia.

Przywracanie urządzeń

Istnieje możliwość przywrócenia jednego lub kilku urządzeń do wcześniej utworzonych punktów przywracania. Aby można było przywrócić urządzenia, dla każdego z nich musi być dostępny co najmniej jeden punkt przywracania. Zgodnie z ustawieniami domyślnymi automatyczne punkty przywracania są tworzone i na bieżąco usuwane co noc dla wszystkich urządzeń na wybranym serwerze. Określona liczba najnowszych automatycznych punktów przywracania jest przechowywana na potrzeby przywracania urządzeń.

Przywracanie urządzeń do wcześniejszego punktu przywracania:

1. Przejdź do obszaru roboczego **Device management (Zarządzanie urządzeniami)**.
2. Wybierz jedno lub kilka urządzeń do przywrócenia.
3. Kliknij prawym przyciskiem myszy i z menu rozwijanego wybierz **Backup / Restore (Kopia zapasowa / przywracanie) > Restore to a Previous Time (Przywróć do wcześniejszego czasu)**.
4. Wybierz punkt przywracania z listy najnowszych dostępnych punktów i kliknij **Next (Dalej)**.
5. Przejrzyj ustawienia każdego urządzenia i kliknij **Finish (Zakończ)**.

Konfiguracja

Tworzenie punktu przywracania

Aby utworzyć ręczny punkt przywracania:

- Przejdź do obszaru roboczego **Device management (Zarządzanie urządzeniami)**.
- Wybierz jedno lub kilka urządzeń do przywrócenia.
- Kliknij prawym przyciskiem myszy i wybierz **Backup / Restore (Kopia zapasowa / przywracanie) > Create Restore Points (Utwórz punkty przywracania)**.
- Wpisz opis identyfikujący punkt przywracania.
- Kliknij **OK**.

Uwaga

Ręcznie utworzone punkty przywracania nie są usuwane automatycznie.

Tworzenie automatycznych punktów przywracania

Jeśli masz więcej niż jeden serwer, wybierz z listy serwerów ten, który chcesz skonfigurować.

- Przejdź do obszaru **Options (Opcje) > Restore point settings (Ustawienia punktu przywracania)**.
- Wybierz **Create restore points automatically (Twórz punkty przywracania automatycznie)**, aby umożliwić automatyczne tworzenie punktów przywracania.
- Wprowadź liczbę automatycznych punktów przywracania, które chcesz zapisać, i kliknij **OK**.

Zarządzanie wieloma poświadczeniami

Ta funkcja udostępnia narzędziu AXIS Device Manager poświadczenia konta administratora urządzeń.

Ręczne wpisywanie poświadczeń urządzeń

Jeśli zdecydujesz się na ręczne wprowadzenie poświadczeń urządzeń, spowoduje to zaktualizowanie poświadczeń w narzędziu AXIS Device Manager w odniesieniu do wybranych urządzeń.

- Wybierz jedno lub więcej urządzeń
- Kliknij prawym przyciskiem myszy i z menu rozwijanego wybierz **Advanced (Zaawansowane) -> Enter Device Credentials (Wprowadź poświadczenia urządzenia)**.

Uwaga

Poświadczenia, których działania na urządzeniu nie da się zweryfikować, nie zostaną zaktualizowane. Dla wszystkich urządzeń uczestniczących w takiej operacji należy użyć tego samego hasła i tej samej nazwy użytkownika.

Używanie pliku CSV na potrzeby różnych poświadczeń

W przypadku korzystania z pliku CSV można użyć oddzielnych haseł i oddzielnych nazw użytkownika dla poszczególnych urządzeń. Wiersze pliku CSV są mapowane na odpowiednie urządzenia w bazie danych narzędzia Axis Device Manager za pomocą adresu MAC, adresu IP lub adresu hosta.

W przypadku korzystania z pliku CSV w interfejsie użytkownika pojawi się prośba o określenie, jak należy interpretować kolumny pliku CSV.

Uwaga

Jak określić, któremu urządzeniu odpowiada wiersz w pliku CSV.

Jedna kolumna pliku CSV musi zawierać adresy MAC, adresy IP lub adresy hostów, więc określ kolumnę w pliku CSV, która ma być interpretowana albo jako adres MAC, albo jako adres IP lub adres hosta. Jest to potrzebne do określenia, któremu urządzeniu odpowiadają dane zawarte w danym wierszu pliku CSV. Dodatkowo można określić kolumnę, która będzie interpretowana jako nazwa serwera. W ten sposób można rozróżnić wiersze zawarte w pliku CSV, które dotyczą urządzeń umieszczonych na różnych serwerach Axis Device Manager, ale mających ten sam adres IP lub adres hosta. Jeśli takie rozróżnienie nie jest wymagane,

nie ma potrzeby wskazywania kolumny, która ma być interpretowana jako nazwa serwera. W konfiguracji, w której serwer korzysta tego samego adresu IP lub adresu hosta dla kilku urządzeń, ale odróżnia je od siebie na podstawie portów, można określić kolumnę, która będzie interpretowana jako port. Jeśli nie jest potrzebne rozróżnianie na podstawie portu, zwykle nie ma powodu, aby interpretować określoną kolumnę jako port. Alternatywą dla podania portu w odrębnej kolumnie jest podanie go razem z adresem IP lub adresem hosta. Wówczas po adresie IP lub adresie hosta należy umieścić dwukropek i numer portu.

Instalowanie certyfikatów

Informacje o certyfikatach

Narzędzie AXIS Device Manager udostępnia ustawienia przeznaczone do zarządzania certyfikatami serwera i klienta. Certyfikaty klienta są używane w przypadku protokołu IEEE 802.1X, a certyfikaty serwera — protokołu HTTPS. Aby wprowadzić ewentualne zmiany, należy wybrać odpowiednie urządzenia w obszarze Device management (Zarządzanie urządzeniami), a następnie wybierać opcję Enable/Update (Włącz/Aktualizuj) w menu kontekstowym.

Tworzenie urzędu certyfikacji (CA)

Funkcja urzędu certyfikacji umożliwia korzystanie z protokołów HTTPS i IEEE 802.1X na urządzeniach, które nie zawierają certyfikatów serwera/klienta. Urząd certyfikacji instruuje urządzenia, aby utworzyły certyfikat przy użyciu własnego klucza prywatnego, podpisały go, a następnie zainstalowały.

Aby utworzyć urząd certyfikacji:

- Przejdź do karty **Configuration (Konfiguracja)**.
- Przejdź do obszaru **Security (Bezpieczeństwo) > Certificates (Certyfikaty)**
- W obszarze **Certificate authority (Urząd certyfikacji)** kliknij **Generate... (Generuj...)**
- Wpisz hasło i zatwierdź je.
- Kliknij **OK**.

Urząd certyfikacji zostanie wygenerowany i będzie gotowy do użycia.

Uwaga

Certyfikat główny z podpisem własnym i klucz prywatny chroniony wybranym hasłem. Certyfikat wygenerowany przez narzędzie AXIS Device Manager będzie ważny przez 3 lata. Jeśli chcesz, aby narzędzie AXIS Device Manager automatycznie odnawiało certyfikaty serwera/klienta, zaznacz pole **Remember passphrase (Zapamiętaj hasło)**. Jeśli urząd certyfikacji nie zostanie skonfigurowany, konieczne będzie tworzenie certyfikatów serwera/klienta poza narzędziem AXIS Device Manager. Utracisz wtedy zalety automatycznego zarządzania certyfikatami.

Import (Importuj) — za pomocą funkcji importu można zaimportować istniejący urząd certyfikacji składający się z certyfikatu publicznego i klucza prywatnego. Konieczne będzie podanie hasła.

Save to file (Zapisz do pliku) — zapisz certyfikat publiczny urzędu certyfikacji w formacie .cer lub .crt. Plik nie będzie zawierał klucza prywatnego, a zatem nie zostanie zaszyfrowany.

Backup (Kopia zapasowa) — zaleca się utworzenie kopii zapasowej urzędu certyfikacji na wypadek awarii sprzętu. W przypadku wybrania tej opcji zostanie utworzona kopia zapasowa zarówno certyfikatu, jak i klucza prywatnego urzędu certyfikacji używanego przez narzędzie Axis Device Manager. Dane kopii zapasowej będą chronione hasłem użytym do wygenerowania urzędu certyfikacji.

Ostrzeżenie o wygaśnięciu certyfikatu Jeśli certyfikat wygaśnie lub będzie się zbliżać termin jego wygaśnięcia, zostanie utworzone powiadomienie systemowe. Dotyczy to wszystkich certyfikatów zainstalowanych na połączonych urządzeniach z wyjątkiem urzędów certyfikacji zainstalowanych poza narzędziem AXIS Device Manager. Ostrzeżenie pojawi się jako alarm systemowy, w kolumnie statusu w obszarze zarządzania urządzeniami, w postaci ikon w oknie dialogowym „View installed certificates (Wyświetl zainstalowane certyfikaty)" oraz w obszarze roboczym konfiguracji.

Określ, z jakim wyprzedzeniem narzędzie AXIS Device Manager ma powiadamiać o zbliżaniu się terminu ważności certyfikatów. Zgodnie z ustawieniem domyślnym certyfikaty serwera i klienta wygenerowane przez

narzędzie AXIS Device Manager są odnawiane automatycznie na siedem dni przed zaplanowanym wyświetleniem ostrzeżenia o wygaśnięciu. Aby otrzymać powiadomienie o zbliżającym się wygaśnięciu urzędu certyfikacji, należy zaznaczyć opcję „remember passphrase (zapamiętaj hasło)".

Włączanie protokołu HTTPS

Aby można było włączyć protokół HTTPS, na każdym urządzeniu musi znajdować się certyfikat serwera. Narzędzie AXIS Device Manager może używać urzędu certyfikacji (CA) w celu podpisywania i instalowania certyfikatów serwera przeznaczonych dla urządzeń.

Można to również zrobić ręcznie:

1. Przejdź do karty **Device manager (Menedżer urządzeń)**
2. Kliknij urządzenia prawym przyciskiem myszy i w menu kontekstowym wybierz **Install server certificates (Zainstaluj certyfikaty serwera)** dla każdego urządzenia.

Przed włączeniem protokołu HTTPS na każdym urządzeniu może znajdować się tylko jeden certyfikat serwera. Nadmiarowe certyfikaty można usunąć przy użyciu menu kontekstowego.

3. Po zainstalowaniu certyfikatów możesz włączyć protokół HTTPS w menu kontekstowym.

Uwaga

Jeśli bezpieczne połączenie (HTTPS) nie jest dostępne, połączenie można nawiązać za pomocą protokołu HTTP. Ma to na celu umożliwienie konfiguracji urządzeń, które jeszcze nie są zabezpieczone.

Ignorowanie weryfikacji certyfikatu

Narzędzie AXIS Device Manager nie połączy się z urządzeniem, jeśli jego certyfikat nie został zweryfikowany. Certyfikat serwera musi zostać podpisany przez aktywny urząd certyfikacji w aplikacji AXIS Device Manager lub zweryfikowany za pośrednictwem magazynu certyfikatów systemu Windows. Po wybraniu opcji Ignore certificate validation (Ignoruj weryfikację certyfikatu) narzędzie AXIS Device Manager nie będzie sprawdzać, czy certyfikat wysłany przez urządzenie jest zaufany czy nie.

Aby narzędzie AXIS Device Manager ignorowało weryfikację certyfikatu:

- Przejdź do karty **Configuration (Konfiguracja)**.
- W obszarze **HTTPS** włącz **Ignore certificate validation (Ignoruj weryfikację certyfikatu)**.

Włączanie protokołu 802.1X

Aby można było włączyć protokół IEEE 802.1X, na każdym urządzeniu musi znajdować się certyfikat klienta. Narzędzie AXIS Device Manager może używać urzędu certyfikacji (CA) w celu podpisywania i instalowania certyfikatów klienta przeznaczonych dla urządzeń.

Czynność tę można również wykonać ręcznie w obszarze zarządzania urządzeniami, klikając urządzenia prawym przyciskiem myszy i wybierając dla każdego z nich opcję instalacji certyfikatów klienta w menu kontekstowym. Przed włączeniem protokołu IEEE 802.1X na każdym urządzeniu może znajdować się tylko jeden certyfikat klienta. Nadmiarowe certyfikaty można usunąć przy użyciu menu kontekstowego. Po zainstalowaniu certyfikatów możesz włączyć protokół IEEE 802.1X w menu kontekstowym.

Do korzystania z protokołu IEEE 802.1X potrzebny jest również certyfikat urzędu certyfikacji do celów uwierzytelniania IEEE 802.1X.

EAPOL Version (Wersja EAPOL) — wybierz wersję protokołu Extensible Authentication Protocol (EAP), której chcesz używać.

EAP identity (Tożsamość EAP) — wprowadź adres MAC urządzenia, nazwę hosta urządzenia lub tekst własny.

Custom (Niestandardowy) — wprowadź dowolny tekst, który będzie służył jako tożsamość EAP.

IEEE 802.1X authentication CA certificate (Certyfikat CA do uwierzytelniania IEEE 802.1X) — oprócz certyfikatu klienta musi być również zainstalowany certyfikat CA na potrzeby uwierzytelniania za pomocą protokołu IEEE 802.1X. Do aktywowania protokołu IEEE 802.1X potrzebny jest tylko certyfikat publiczny, a nie klucz prywatny,

więc nie ma potrzeby stosowania hasła. Certyfikat CA uwierzytelniania w standardzie IEEE 802.1X zostanie zainstalowany podczas włączania lub aktualizowania oprogramowania protokołu IEEE 802.1X..

Import (Importuj) — wybierz certyfikat CA, który zostanie zainstalowany na urządzeniach i posłuży do weryfikacji serwera uwierzytelniania. Certyfikat CA może zostać utworzony przez urząd certyfikacji (CA) w narzędziu AXIS Device Manager lub pochodzić ze źródła zewnętrznego.

View (Wyświetl) — szczegóły certyfikatu CA używanego podczas uwierzytelniania IEEE 802.1X.

Common name (Nazwa pospolita) — wybierz tożsamość EAP urządzenia lub jego adres IP. Jeśli pole Custom (Niestandardowy) pozostanie puste, zostanie wybrana nazwa hosta. Jeśli wystąpi problem z nazwą hosta, jako nazwa pospolita zostanie użyty adres IP.

Zarządzanie kontami SIP

Zarządzanie oprogramowaniem urządzeń

Aktualizacje systemu AXIS OS

Nowe wersje systemu AXIS OS można uzyskać na dwa sposoby:

- Pobrać za pomocą narzędzia AXIS Device Manager (wymaga dostępu do Internetu)
- Zaimportować z pliku (np. z dysku twardego lub USB).

Uwaga

Zachęcamy do przestrzegania zalecanej ścieżki aktualizacji systemu AXIS OS. Więcej na ten temat można przeczytać tutaj: *https://help.axis.com/axis-os#upgrade-path*

Ręczna aktualizacja systemu AXIS OS

1. Wybierz urządzenia, które chcesz zaktualizować do nowej wersji systemu AXIS OS, kliknij prawym przyciskiem myszy i wybierz **Upgrade AXIS OS (Aktualizuj system AXIS OS)**.
2. W oknie dialogowym **Upgrade firmware (Aktualizowanie oprogramowania sprzętowego)**: Aby zaktualizować listę wersji oprogramowania sprzętowego możliwych do pobrania, kliknij przycisk **Check now** (Sprawdź teraz).
3. Aby wyszukać jeden lub więcej plików wersji systemu AXIS OS przechowywanych na kliencie lokalnym, kliknij przycisk **Browse (Przeglądaj)**.
4. Aby przywrócić ustawienia fabryczne wybranych urządzeń podczas aktualizowania systemu AXIS OS, kliknij pole wyboru **Factory default (Ustawienia fabryczne)**. Jest to wymagane w przypadku obniżania niektórych wersji systemu AXIS OS.
5. Wybierz urządzenia i wersje systemu AXIS OS, które chcesz zaktualizować, oraz kliknij **OK**, aby rozpocząć aktualizowanie urządzeń wybranych z listy.

Uwaga

Domyślnie aktualizacje systemu AXIS OS odbywają się na wszystkich wybranych urządzeniach równocześnie. Kolejność aktualizacji można zmienić w obszarze **Configuration (Konfiguracja) > Connected Services (Połączone usługi) > Firmware upgrade settings (Ustawienia aktualizacji oprogramowania sprzętowego)**.

Aktualizacje automatyczne

Zgodnie z ustawieniem domyślnym narzędzie AXIS Device Manager 5 nie sprawdza dostępności aktualizacji systemu AXIS OS, ale można je skonfigurować tak, aby automatycznie sprawdzało, czy są dostępne aktualizacje systemu AXIS OS na serwerze lub na stronie axis.com.

Aby ręcznie sprawdzić dostępność aktualizacji systemu AXIS OS, naciśnij przycisk **Check now (Sprawdź teraz)** w menu akcji.

Kolejność aktualizacji systemu AXIS OS

Aktualizacje systemu AXIS OS mogą być wykonywane na wszystkich urządzeniach jednocześnie lub kolejno na poszczególnych urządzeniach.

- Aby zaktualizować wszystkie urządzenia jednocześnie, wybierz kolejność aktualizacji **Parallel (Równolegle)**.
- Aby zaktualizować urządzenia jedno po drugim, wybierz **Sequential (Sekwencyjnie)**. Ta opcja wymaga więcej czasu, ale urządzenia nie będą się znajdować w trybie offline jednocześnie. Można również spowodować zatrzymanie aktualizacji sekwencyjnej w przypadku wystąpienia problemu, zaznaczając pole **Cancel all remaining upgrades if one device fails (Anuluj wszystkie pozostałe aktualizacje, jeśli na jednym urządzeniu wystąpi niepowodzenie**.

Rozwiązywanie problemów

Kontakt z pomocą techniczną

Kontaktując się z pomocą techniczną, należy najpierw utworzyć zgłoszenie i załączyć plik raportu systemowego, aby ułatwić rozwiązanie danego problemu:

1. Wejdź do menu głównego.
2. Przejdź do obszaru **Help (Pomoc) > System Report... (Raport systemowy...)**
3. Zapisz plik raportu w wybranym folderze.
4. Przejdź na stronę *axis.com/support*.
5. Utwórz zgłoszenie do pomocy technicznej.
6. Załącz plik do utworzonego zgłoszenia do pomocy technicznej.

Uwaga

Aby utworzyć raport systemowy z niereagującego systemu:

1. Przejdź do `C:\ProgramData\Axis Communications\`
2. Zarchiwizuj zawartość folderu do pliku .zip i dołącz go do zgłoszenia do pomocy technicznej.

Proces eskalacji

W przypadku wystąpienia problemów, których nie można rozwiązać za pomocą tego przewodnika, zgłoś problem do internetowego punktu pomocy technicznej Axis, patrz *Internetowy punkt pomocy technicznej Axis*. Aby nasz zespół pomocy technicznej mógł zrozumieć i rozwiązać Twój problem, musisz podać następujące informacje:

- Jasny opis, jak odtworzyć problem lub okoliczności, w jakich występuje.
- Godzina i nazwa lub adres IP urządzenia, w którym występuje problem.
- AXIS Device Manager : raport systemowy generowany bezpośrednio po wystąpieniu problemu. Raport systemowy musi zostać wygenerowany przez klienta lub serwer, na którym odtworzono problem.
- Opcjonalne zrzuty ekranu lub nagrania przedstawiające problem.
- W razie potrzeby dołącz pliki bazy danych. Aby przyspieszyć przesyłanie, możesz je pominąć.

Niektóre problemy wymagają podania dodatkowych informacji, których zespół pomocy technicznej zażąda w razie potrzeby.

Uwaga

Jeśli rozmiar pliku (na przykład ślad sieciowy lub plik bazy danych) przekracza 100 MB, użyj zaufanej usługi bezpiecznego udostępniania plików.

Informacje dodatkowe	
Dzienniki poziomu debugowania	Czasami używamy dzienników poziomu debugowania do zebrania większej ilości informacji. Odbywa się to wyłącznie na żądanie inżyniera pomocy technicznej firmy Axis. Instrukcje można znaleźć w *internetowym centrum pomocy technicznej Axis*.
Ślad sieciowy	Jeśli poprosi o to inżynier pomocy technicznej, wygeneruj ślady sieciowe podczas tworzenia raportu systemowego. Wykonaj ślady sieciowe w czasie, gdy występuje problem, jeśli jest to proces, który da się odtworzyć. Obejmuje to: • 60-sekundowy ślad sieciowy zarejestrowany kamerą (dotyczy tylko oprogramowania sprzętowego w wersji 5.20 i nowszych) W razie potrzeby użyj następującego polecenia VAPIX, aby zmienić login, adres IP i czas trwania (w sekundach):

Informacje dodatkowe	
	`http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • 10–30-sekundowy ślad sieciowy na serwerze, ukazujący komunikację między serwerem a kamerą.
Pliki baz danych	W przypadkach, gdy musimy sprawdzić lub ręcznie naprawić bazę danych. Przed wygenerowaniem raportu systemowego zaznacz opcję **Include database in the report (Dołącz bazę danych do raportu)**.
Zrzuty ekranu	Użyj zrzutów ekranu, jeśli problem podglądu na żywo jest związany z interfejsem użytkownika. Na przykład, gdy chcesz pokazać oś czasu nagrań lub gdy trudno opisać problem.
Nagrania ekranu	Użyj nagrań ekranu, jeśli trudno jest opisać problem słowami, na przykład gdy odtworzenie problemu wymaga wiele interakcji z interfejsem użytkownika.

T10211981_pl

2025-08 (M2.2)